PAGE A9

WASHINGTON POST
11 April 1987

Eavesdropping Becomes Undetectable

Lasers, Cloaked Transmissions Employed in Advanced Espionage

By Michael Specter
Washington Post Staff Writer

Whether dangling invisibly from hidden ceilings or molded to the face of a clock, listening devices have become so sophisticated that many security specialists say the best of them seem invincible.

"As far as I am concerned the embassy in Moscow is completely compromised," said Gregory Stone, a consultant on electronic surveillance. "If they planted their bugs properly, you could tear the building down and nobody would find them."

What has been good for consumer electronics has been great for spies. Using a mix of lasers, pin-sized transmitters and computers capable of separating a quiet conversation from a roar of sound, Soviet and U.S. espionage specialists employ an array of bugs that only 10 years ago would have seemed suited for science fiction.

The most common bugs, and the easiest to detect, essentially are radios that transmit to nearby receivers.

More complicated eavesdropping devices, called parasitic transmitters, can be planted in a power line. Using electricity from the line, they send signals to distant locations.

"Most of that stuff can be picked off without any real problem," said Dick Heffernan, vice president of Information Security Associates Inc. (ISA), which specializes in equipment to detect bugs. "It's a real nuisance and you have to be very careful, but it's not going to work on a U.S. embassy."

To find a bug, ISA and others use spectrum analysis, which measures radio frequencies in a room. When they find a strange frequency, they can zero in on it.

The most advanced bug-detecting machines are called nonlinear junction detectors. This is a box that beams microwaves at surfaces that may have been bugged, to pick up transmitting signals.

"You have to use a real mix of high-tech and low-tech to find these things," said Francis Mason, who runs an engineering concern that specializes in devices that detect bugs. "You need a whole mix of technologies. Sometimes you have to take every piece of machinery in a room apart by hand."

Lasers and a sophisticated technique called spread spectrum transmission are harder to detect. A laser can bounce a light beam against a window, picking up the slightest vibrations on the glass of a room where people are talking. The beam, packed with sound, then heads back to a computer which can analyze the contents and recompose what was said.

But lasers have their drawbacks, too. Companies now sell small electric motors that can be attached to windows to produce vibrations that usually throw off even the most sophisticated computers.

But the state of the art, according to several security experts, is spread spectrum transmission. In a normal bug, the signal is transmitted on a single, detectable wavelength.

A spread spectrum listening device works on the same transmitting principle but disperses its signal across a wide band of radio frequencies.

"If you tune in with an agile receiver, you would see a big blip where the conventional bug is sending its message," Stone said. "But the spread signal sends far less power over a very wide space. Even the most sensitive devices can't detect it."

When the information has been received, an advanced detection system picks it up, amplifies all the sound waves and turns them into digital signals. The computer then throws away the meaningless noise, extracts the useful sound—or video images—and translates it.

The most sophisticated devices, such as spread spectrum transmitters and decoders, cost millions of dollars. The technology is not available to commercial consumers.

Among other bugging methods are devices that send information through wires in brief bursts that are rarely detected, and new ways to translate information passing along fiber optic cables.